AO 93 (Rev. 11/13) Search and Seizure Warrant

FILED

MAR 18 2020

U. S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE CELLULAR PHONE NUMBER [redacted] THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.

Case No. 4:20 MJ 77 DDN

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the NORTHERN District of CALIFORNIA
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

YOU ARE COMMANDED to execute this warrant on or before April 1, 2020 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable David D. Noce
(United States Magistrate Judge).

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying the later specific date of ____.

Date and time issued: 8:30 am March 18, 2020

David D. Noce
Judge's signature

City and state: St. Louis, MO

Honorable David D. Noce, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the cellular phone number [redacted] (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from January 1, 2019 to March 18, 2020, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account January 1, 2019 to March 18, 2020, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of Title 18, United States Code, Sections 666, 1341, 1343, and 1346 involving John Collins-Muhammad from January 1, 2019 to March 18, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters: communications between John Collins-Muhammad and CW1 or other business owners; the receipt of anything of value in exchange for official action; communications between John Collins-Muhammad and other public officials regarding CW1 or other business owners; communications with employees of the City of St. Louis regarding CW1 or other business owners; communications between John Collins-Muhammad and other public officials regarding a scheme to deprive the citizens of St. Louis, Missouri of their right to honest services; and;

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **[PROVIDER]**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **[PROVIDER]**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **[PROVIDER]**, and they were made by **[PROVIDER]** as a regular practice; and

b. such records were generated by **[PROVIDER'S]** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **[PROVIDER]** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **[PROVIDER]**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES DISTRICT COURT

FILED

MAR 18 2020

U. S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

for the

Eastern District of Missouri

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH THE CELLULAR PHONE NUMBER [redacted] THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.

Case No. 4:20 MJ 77 DDN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 666	Theft or bribery concerning programs receiving Federal funds
18 U.S.C. Section 1346	Honest Services Fraud
18 U.S.C. Section 1341	Frauds and Swindles
18 U.S.C. Section 1343	Wire Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth [redacted]

[redacted]
Applicant's signature

[redacted]
Printed name and title

Sworn to before me and signed in my presence.

Date: March 18, 2020

David D. Noce
Judge's signature

City and state: St. Louis, MO

Honorable David D. Noce, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR PHONE NUMBER [redacted] THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	)	No. 4:20 MJ 77 DDN FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent [redacted], a Special Agent with the Federal Bureau of Investigation, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Apple Inc. (hereafter "Apple"), an electronic communications service/remote computing service provider, to disclose to the United States records and other information, including the contents of communications, associated with John Collins-Muhammad and cellular phone number [redacted] that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been so employed since 2002. I am presently assigned to the Public Corruption squad in the St. Louis Division of the FBI. My responsibilities include the investigation of federal crimes to include violations of Title 18 United States Code (U.S.C.) § 666 (Theft or bribery concerning programs receiving Federal funds), § 1346 (Honest Services Fraud), § 1341 (Mail Fraud) and § 1343 (Wire

Fraud). I am currently assigned to investigate allegations of public corruption. I received over eighteen weeks of specialized law enforcement training at the FBI Academy in Quantico, Virginia. My experience obtained as a Special Agent of the FBI has included investigations of multiple violations of federal criminal public corruption laws. I know cellular telephones are commonly used by politicians to communicate with donors, constituents, and employees. Cellular telephones enable a politician to communicate during the day when they are not at an office location, which is common with this type of work. Cellular telephones also enable the user to quickly send text messages to other people when they are unable to take the time to make a phone call, but the sender needs to quickly convey their message.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. Section 666 (Theft or bribery concerning programs receiving Federal funds), 18 U.S.C. Section 1346 (Honest Services Fraud), or 18 U.S.C. Sections 1341 and 1343 (Mail and Wire Fraud) have been committed by John Collins-Muhammad, a St. Louis, Missouri Alderman. There is also probable cause to search the information described in Attachment A for evidence of these crimes (as described in Attachment B).

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).]

LOCATION TO BE SEARCHED

6. The location to be searched is:

The cellular phone number [redacted] (hereinafter referred to as "the account") located at a premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

BACKGROUND INFORMATION RELATING TO APPLE ID AND iCLOUD[1]

7. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

8. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages")

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

9. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

10. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in@icloud.com, @me.com, or@mac.com) or an email address associated with a third- party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

11. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including

the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

12. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

13. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer

is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

14. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

15. The United States is investigating allegations that St. Louis City Alderman John Collins-Muhammad is accepting bribe payments from local businessmen in exchange for taking official action relative to property tax abatements, liquor licenses, and other business licenses.

The allegations disclose possible violations of 18 U.S.C. Sections 666, 1341, 1343, and 1346. In my training and experience, evidence of who was using an Apple ID, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

16. As stated below, John Collins-Muhammad sent text messages and iMessages related to the taking of official action relative to the awarding of property tax abatements, liquor licenses, and other city licenses. Stored communications and files from the account that is the subject of this affidavit are vital to this ongoing investigation. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, including with this investigation, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

17. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device

identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

18. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

19. As stated below, the investigation to date has revealed that John Collins-Muhammad sent text messages and iMessages to CW1 and others related to the awarding of property tax abatements and other City licenses. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co- conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

20. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

PROBABLE CAUSE

21. The FBI opened a formal investigation of St. Louis' 21st Ward Alderman John Collins-Muhammad on [redacted]. A cooperating witness (CW1) provided information to

the FBI as part of a proffer agreement. CW1 and his brothers operate several gas stations and convenience stores in the City of St. Louis, including in the 21st Ward. CW1 provided information on bribe payments and kickbacks to several St. Louis City Aldermen, St. Louis City officials, and [redacted], including Alderman Collins-Muhammad. During the course of proffer sessions with the Government in [redacted], CW1 stated that Alderman Collins-Muhammad (hereinafter referred to as "JCM") shut down a store owned and operated by [redacted], an associate of CW1, in the 21st Ward in the City of St. Louis. In shutting down the store, JCM alleged various city violations in the operation of the store. A close associate of CW1 spoke with JCM in order to facilitate the payment of a bribe between [redacted] and JCM in the amount of approximately $2,500 in order to get the store reopened. [redacted] handed the cash to CW1's associate and CW1's associate then handed it over to JCM. Shortly after [redacted] paid the cash bribe to JCM, JCM caused the purported violations to be expunged, and [redacted] was allowed to reopen his store.

22. On or about January 16, 2020, CW1 called JCM on telephone [redacted] (hereinafter referred to as [redacted]) to arrange a meeting. On January 18, 2020, JCM came to one of CW1's stores. During the first minute of their meeting, CW1 stated, "If you could help it would be phenomenal." JCM replied, "Tell me what you need." CW1 then detailed items such as liquor licenses and property tax abatements that would help his businesses in JCM's and other St. Louis City wards. JCM told CW1, "I can take care of you in my Ward." JCM made other assurances to CW1 that he could assist with a property tax abatement for his store over a ten year period by submitting a letter in support which was necessary to receive such an abatement. JCM also told CW1 if the abatement approval was taking too long, JCM would help move it along. JCM told

CW1 the annual property taxes on the property were approximately $17,000. This meeting was recorded.

23. On or about January 20, 2020, JCM sent a text message from [redacted] to CW1 stating, in part, "I got your letter of approval for tax abatement."

24. On January 21, 2020, JCM brought the tax abatement forms and his letter of support to CW1. JCM provided the name of the St. Louis City employee who CW1 was to submit the completed forms to. Also during this meeting, CW1 told JCM the savings related to this property tax abatement amounted to approximately $130,000 over 10 years. This meeting was recorded.

25. On January 24, 2020, JCM met with CW1 to ask about the status of the tax abatement paperwork. During this meeting, JCM discussed other deals he could assist CW1 with, including introducing CW1 to another City Alderman in a different Ward where CW1 owned and operated a business. At the end of this meeting, CW1 asked JCM, "What do I owe you for this?" JCM stated, "25". JCM stated he would return at 4:00 pm that day to get the money. This meeting was recorded.

26. JCM returned to CW1's store at approximately 4:00 pm on January 24, 2020. During their meeting, CW1 gave JCM $2,500 cash, which JCM immediately placed into his front-right jacket pocket. CW1 thanked JCM for his help on obtaining the property tax abatement, to which JCM replied, "That's our job. That's the job for an alderman." This meeting was recorded.

27. On or about January 31, 2020, JCM met with CW1. During the meeting, CW1 gave JCM a check for the City for the administrative charges related to the property tax abatement application. JCM told CW1 the paperwork CW1 gave JCM looked good and the approval would take about one week. JCM told CW1, once approved by the City, the property would receive favorable tax abatement treatment from 2021-2030. This meeting was recorded. During that same

January 31, 2020 meeting with JCM, CW1 asked JCM how CW1 should approach [redacted], another St. Louis City Alderman, in order to get a similar property tax abatement Aldermanic support letter for a different property in [redacted] Ward. During that discussion, JCM described how CW1 should make the [bribe] payment to [redacted] - using an intermediary. JCM told CW1 to bring [redacted] assistant, in to "do some bullshit consulting". JCM then suggested $5,000 for the "consulting" in exchange for the property tax abatement support letter, which he then lowered to $3,000, saying anything would help. JCM explained [redacted] needed the money, stating she had not paid her own personal property taxes. JCM then assured CW1 that JCM told [redacted], "We're good," which was understood to mean both aldermen and CW1 were all on the same page regarding the payment and acceptance of money for official action. JCM told CW1 that [redacted] "does business under the table". This meeting was recorded.

28. Later that same day, on January 31, 2020, CW1 met with [redacted], after JCM made an introduction between the two. CW1 and [redacted] discussed that [redacted] would provide an Aldermanic letter of support for a 15 year property tax abatement for CW1's business in [redacted] Ward. During this meeting, [redacted] directed the Board of Alderman secretary to prepare the letter for CW1. CW1 then offered $2,000 cash to [redacted] in exchange for the Aldermanic letter of support, and [redacted] directed CW1 to make the payment to [redacted], his assistant. [redacted] told CW1 that [redacted] was currently down the street at a beauty shop, and CW1 should take the money to [redacted] there. As CW1 left the meeting, he told [redacted] that he was going to give [redacted] "2," meaning $2,000. This meeting was recorded. CW1 left the meeting with [redacted] and traveled to the beauty shop where he met with [redacted]. CW1 paid [redacted] $2,000 in cash at that time. This meeting was recorded.

29. On or about February 6, 2020, JCM told CW1 about a dispute he was having with [redacted], a convenience store owner in JCM's Ward. The nature of the dispute had to do with the convenience store having unpaid fines and possibly some permitting issues. JCM told CW1 the City was poised to close the business, and only JCM, as the Alderman, could prevent the business from closing. JCM accepted CW1's offer to be an intermediary on behalf of JCM and [redacted] On February 6, 2020, JCM sent CW1 a text message from [redacted] with [redacted] telephone number in order for CW1 to contact [redacted]

30. CW1 then recorded his conversations with [redacted] and his business partners while they discussed the historical and current demands from JCM for money in order to stay open. While acting as the intermediary, [redacted] revealed to CW1 on February 7, 2020 the control JCM has over his store, and the fact that JCM had demanded between $5,000-$7,000 from [redacted] relative to the store's operations. [redacted] asked CW1, "Where does he [JCM] think we are? Our gas station does not have liquor or anything; we are barely making ends meet."

31. On February 8, 2020, JCM sent a text to CW1 from [redacted] stating [redacted] "hasn't called me yet." JCM then sent a text two hours later to CW1 from [redacted] that read, "He plays me; thats (sic) bad business." On February 8, 2020, [redacted] told CW1 in a recorded conversation that JCM started to call him at all hours to shut down his business; and that he wants $5,000 to let the business stay open. CW1 asked [redacted] if JCM contacted him that day, and [redacted] said that he did. [redacted] also said that JCM keeps on threatening him by phone and text messages about shutting down the gas station. [redacted] explained that he had already paid JCM $200, $300, $400, and [redacted] business partner gave JCM $600 three or four months ago. [redacted] then said they are paying him [JCM] all the time. A Court ordered pen register showed multiple calls and text messages from JCM to [redacted] on [redacted] during this timeframe.

32. Shortly thereafter, JCM abruptly told CW1 to stop acting as the intermediary, but then on February 12, 2020, the discussion resumed when a different business partner of [redacted] got involved. This business partner understood that while the bribe payments should not occur, if they wanted to continue to operate a business in JCM's Ward, they needed to make the payments. In a recorded conversation, CW1 asked JCM what CW1 should say to the other business partner. JCM said, "$2,500 Friday; another $2,500 in a few weeks." CW1 asked who they should give the money to and JCM told CW1 they could give the money directly to CW1. It was clear from the conversation that the $5,000 will go to JCM and is not intended for the payment of any legitimate City fines or taxes.

33. In recorded conversations, JCM has offered to connect CW1 with two other local politicians who could use their public offices to help CW1 and his businesses. CW1 talked to JCM about giving money to these politicians in exchange for their official action. CW1 observed JCM using the Apple text messenger on [redacted] to communicate with one of these politicians while he was in a meeting with JCM. JCM used Apple text messenger on March 6, 2020 to tell CW1 he had not forgotten to schedule the meeting with that particular politician and that he "will take care of everything". CW1 has not yet met with either of the politicians as of the date of this application.

34. A review of a court authorized pen register on [redacted] identified between [redacted], JCM sent and received a total of 619 text messages – an average of over 44 text messages a day. The FBI assesses there are even more messages that were not identified in the pen register based on the Apple to Apple iMessages that do not appear on the pen register.

35. Based on my training and experience, I know that text messages sent between JCM and others were sent and received on Apple devices based on a review of several text messages

provided by CW1. I am also aware many Apple device owners utilize a cloud-based backup and storage service, which captures text messages. Two preservation requests were sent to Apple, Inc. for JCM's cellular phone number [redacted], on [redacted].

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

36. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the United States copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

39. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their

premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

[redacted]

Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on March 18, 2020

David D. Noce

DAVID D. NOCE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the cellular phone number [redacted] (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from January 1, 2019 to March 18, 2020, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account January 1, 2019 to March 18, 2020, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of Title 18, United States Code, Sections 666, 1341, 1343, and 1346 involving John Collins-Muhammad from January 1, 2019 to March 18, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters: communications between John Collins-Muhammad and CW1 or other business owners; the receipt of anything of value in exchange for official action; communications between John Collins-Muhammad and other public officials regarding CW1 or other business owners; communications with employees of the City of St. Louis regarding CW1 or other business owners; communications between John Collins-Muhammad and other public officials regarding a scheme to deprive the citizens of St. Louis, Missouri of their right to honest services; and;

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **[PROVIDER]**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **[PROVIDER]**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **[PROVIDER]**, and they were made by **[PROVIDER]** as a regular practice; and

b. such records were generated by **[PROVIDER'S]** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **[PROVIDER]** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **[PROVIDER]**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
4:20 MJ 77 DDN	March 18, 2020 10:38 AM	Emailed to subpoenas@apple.com

Inventory made in the presence of: N/A

Inventory of the property taken and name of any person(s) seized:

Apple provided an email with a link to the file for the search return on 3/26/2020.

FBI downloaded the file from Apple and began the decryption process.

The file was sent to FBI Headquarters for final decryption and processing to a format suitable for review.

On September 1, 2020, this warrant return was submitted by reliable electronic means to the undersigned U.S. Magistrate Judge who signed and issued it in the referenced case. By reliable electronic means this returned warrant is forwarded to the Clerk of Court for filing, with a copy to the officer who returned it. /s/ David D. Noce, U.S. Magistrate Judge, E. D. Mo., September 1, 2020.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 4/13/2020

[redacted]

Executing officer's signature

[redacted]

Printed name and title